

**UNITED STATES DEPARTMENT  
OF  
AGRICULTURE  
NATIONAL FINANCE CENTER**

**PUBLIC KEY INFRASTRUCTURE  
CERTIFICATE POLICY (CP)**

*Version 1.1*

**July 2002**

Confidential

© United States Department of Agriculture  
National Finance Center, 2002



<b>1.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>1.1</b>	<b>OVERVIEW.....</b>	<b>1</b>
1.1.1	Certificate Policy (CP) .....	1
1.1.2	Relationship Between the USDA/NFC CA CP and the USDA/NFC CA CPS .....	2
<b>1.2</b>	<b>IDENTIFICATION.....</b>	<b>2</b>
<b>1.3</b>	<b>COMMUNITY AND APPLICABILITY.....</b>	<b>2</b>
1.3.1	PKI Authorities .....	2
1.3.2	Related Authorities .....	4
1.3.3	End Entities.....	4
1.3.4	Applicability.....	5
<b>1.4</b>	<b>CONTACT DETAILS.....</b>	<b>6</b>
<b>2.</b>	<b>GENERAL PROVISIONS.....</b>	<b>8</b>
<b>2.1</b>	<b>OBLIGATIONS.....</b>	<b>8</b>
2.1.1	CA Obligations .....	8
2.1.2	RA or LRA Obligations .....	8
2.1.3	Subscriber Obligations .....	8
2.1.4	Subscriber Organization Obligations .....	9
2.1.5	Repository Obligations .....	9
2.1.6	Certificate Issuance to Non-US Government Parties.....	9
<b>2.2</b>	<b>LIABILITY.....</b>	<b>9</b>
<b>2.3</b>	<b>FINANCIAL RESPONSIBILITY.....</b>	<b>9</b>
2.3.1	Indemnification by Relying Parties and Subscribers .....	9
2.3.2	Fiduciary Relationships .....	10
2.3.3	Administrative Processes .....	10
<b>2.4</b>	<b>INTERPRETATION AND ENFORCEMENT.....</b>	<b>10</b>
2.4.1	Agency Policy.....	10
2.4.2	Governing Law .....	10
2.4.3	Severability of Provisions, Survival, Merger, and Notice .....	10
2.4.4	Dispute Resolution Procedures .....	10
<b>2.5</b>	<b>FEES.....</b>	<b>10</b>
<b>2.6</b>	<b>PUBLICATION AND REPOSITORY.....</b>	<b>11</b>
2.6.1	Publication of CA Information .....	11
2.6.2	Frequency of Publication.....	11
2.6.3	Access Controls .....	11
2.6.4	Repositories.....	11

<b>2.7</b>	<b><i>COMPLIANCE AUDIT</i></b> .....	<b>11</b>
2.7.1	Frequency of Entity Compliance Audit .....	11
2.7.2	Identity/Qualifications of Compliance Auditor .....	12
2.7.3	Compliance Auditor's Relationship to Audited Party .....	12
2.7.4	Topics Covered by Compliance Audit.....	12
2.7.5	Actions Taken as a Result of Deficiency.....	12
2.7.6	Communication of Result .....	13
<b>2.8</b>	<b><i>CONFIDENTIALITY</i></b> .....	<b>13</b>
<b>2.9</b>	<b><i>INTELLECTUAL PROPERTY RIGHTS</i></b> .....	<b>13</b>
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION</b> .....	<b>14</b>
<b>3.1</b>	<b><i>INITIAL REGISTRATION</i></b> .....	<b>14</b>
3.1.1	Types of Names .....	14
3.1.2	Need for Names to be Meaningful .....	14
3.1.3	Rules for Interpreting Various Name Forms .....	14
3.1.4	Uniqueness of Names.....	15
3.1.5	Name Claim Dispute Resolution Procedure .....	15
3.1.6	Recognition, Authentication and Role of Trademarks .....	15
3.1.7	Method to Prove Possession of Private Key .....	15
3.1.8	Authentication of Organizational Identity .....	16
3.1.9	Authentication of Individual Identity.....	16
3.1.10	Authentication of Component Identities .....	17
<b>3.2</b>	<b><i>CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY</i></b> .....	<b>17</b>
3.2.1	Certificate Re-key .....	17
3.2.2	Certificate Renewal.....	18
3.2.3	Certificate Update .....	18
<b>3.3</b>	<b><i>OBTAINING A NEW CERTIFICATE AFTER REVOCATION</i></b> .....	<b>19</b>
<b>3.4</b>	<b><i>REVOCATION REQUEST</i></b> .....	<b>19</b>
<b>4.</b>	<b>OPERATIONAL REQUIREMENTS</b> .....	<b>20</b>
<b>4.1</b>	<b><i>APPLICATION FOR A CERTIFICATE</i></b> .....	<b>20</b>
4.1.1	Delivery of Public Key for Certificate Issuance .....	20
<b>4.2</b>	<b><i>CERTIFICATE ISSUANCE</i></b> .....	<b>20</b>
4.2.1	Delivery of Subscriber's Private Key to Subscriber.....	21
4.2.2	USDA/NFC CA Public Key Delivery and Use .....	21
<b>4.3</b>	<b><i>CERTIFICATE ACCEPTANCE</i></b> .....	<b>21</b>
<b>4.4</b>	<b><i>CERTIFICATE REVOCATION</i></b> .....	<b>22</b>

4.4.1	Circumstances for Revocation of a Certificate Issued by the USDA/NFC CA.....	22
4.4.2	Who can Request Revocation of a Certificate Issued by the USDA/NFC CA.....	22
4.4.3	Procedure for Revocation Request.....	22
4.4.4	Revocation of a Certificate Issued by the USDA/NFC CA.....	23
4.4.5	Revocation Request Grace Period.....	23
4.4.6	Certification Authority Revocation Lists / Certificate Revocation Lists .....	23
4.4.7	CRL Issuance Frequency .....	23
4.4.8	CRL Checking Requirements .....	24
4.4.9	On-line Revocation / Status Checking Availability.....	24
4.4.10	Other Forms of Revocation Advertisements Available .....	24
4.4.11	Checking Requirements for Other Forms of Revocation Advertisements .....	24
4.4.12	Special Requirements Related to Key Compromise .....	24
<b>4.5</b>	<b><i>SECURITY AUDIT PROCEDURE</i></b> .....	<b>24</b>
4.5.1	Types of Events Recorded .....	25
4.5.2	Frequency of processing data.....	30
4.5.3	Retention Period for Security Audit Data .....	30
4.5.4	Protection of Audit Log .....	31
4.5.5	Security Audit Data Backup Procedures.....	31
4.5.6	Security Audit Collection System (Internal vs. External) .....	31
4.5.7	Notification to Event-causing Subject .....	31
4.5.8	Vulnerability Assessments .....	31
<b>4.6</b>	<b><i>RECORDS ARCHIVAL</i></b> .....	<b>31</b>
4.6.1	Types of Events Archived.....	31
4.6.2	Retention Period for Archive .....	32
4.6.3	Protection of Archive .....	33
4.6.4	Archive Backup and Management .....	33
4.6.5	Requirements for Time-stamping of Records .....	33
4.6.6	Procedures to Obtain and Verify Archive Information.....	33
<b>4.7</b>	<b><i>KEY CHANGEOVER</i></b> .....	<b>33</b>
<b>4.8</b>	<b><i>COMPROMISE AND DISASTER RECOVERY</i></b> .....	<b>34</b>
4.8.1	Computing Resources, Software, and/or Data are Corrupted .....	34
4.8.2	USDA/NFC CA Signature Keys are Revoked.....	34
4.8.3	USDA/NFC CA Signature Keys are Compromised .....	34
4.8.4	Secure Facility Impaired After a Natural or Other type of Disaster .....	35

<b>4.9</b>	<b><i>CA TERMINATION</i></b> .....	<b>35</b>
<b>5.</b>	<b>PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS</b> .....	<b>36</b>
<b>5.1</b>	<b><i>PHYSICAL CONTROLS FOR THE USDA/NFC CA OR AGENCY CA</i></b> .....	<b>36</b>
5.1.1	Site Location and Construction.....	36
5.1.2	Physical Access.....	36
5.1.3	Electrical Power .....	37
5.1.4	Water Exposures .....	37
5.1.5	Fire Prevention and Protection.....	37
5.1.6	Media Storage .....	38
5.1.7	Waste Disposal.....	38
5.1.8	Off-site Backup .....	38
<b>5.2</b>	<b><i>PROCEDURAL CONTROLS FOR THE USDA/NFC CA</i></b> .....	<b>38</b>
5.2.1	Trusted Roles .....	38
5.2.2	Separation of Roles .....	40
5.2.3	Number of Persons Required Per Task .....	41
5.2.4	Identification and Authentication for Each Role .....	41
<b>5.3</b>	<b><i>PERSONNEL CONTROLS</i></b> .....	<b>41</b>
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements ....	41
5.3.2	Background Check Procedures .....	41
5.3.3	Training Requirements.....	41
5.3.4	Retraining Frequency and Requirements .....	42
5.3.5	Job Rotation Frequency and Sequence .....	42
5.3.6	Sanctions for Unauthorized Actions .....	42
5.3.7	Contracting Personnel Requirements.....	42
5.3.8	Documentation Supplied to Personnel.....	42
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS</b> .....	<b>43</b>
<b>6.1</b>	<b><i>KEY PAIR GENERATION AND INSTALLATION</i></b> .....	<b>43</b>
6.1.1	USDA/NFC CA and CA Key Pair Generation.....	43
6.1.2	Private Key Delivery to Subscriber .....	43
6.1.3	Public Key Delivery to Certificate Issuer .....	43
6.1.4	USDA/NFC CA Public Key Delivery to Subscriber Certificate Holder's .....	43
6.1.5	Key Sizes.....	43
6.1.6	Public Key Parameters Generation.....	44

6.1.7	Parameter Quality Checking .....	44
6.1.8	Hardware/Software Subscriber Key Generation.....	44
6.1.9	Key Usage Purposes (as per X.509 v3 key usage field) .....	44
<b>6.2</b>	<b><i>PRIVATE KEY PROTECTION</i></b> .....	<b>44</b>
6.2.1	Standards for Cryptographic Module .....	44
6.2.2	USDA/NFC CA Private Key Multi-person Control .....	45
6.2.3	Key Escrow of USDA/NFC CA Private Signature Key.....	45
6.2.4	Private Key Backup .....	45
6.2.5	Private Key Archival.....	46
6.2.6	Private Key Entry into Cryptographic Module .....	46
6.2.7	Method of Activating Private Keys .....	46
6.2.8	Methods of Deactivating Private Keys .....	46
6.2.9	Method of Destroying Subscriber Private Signature Keys .....	46
<b>6.3</b>	<b><i>GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT</i></b> .....	<b>46</b>
6.3.1	Public Key Archival.....	46
6.3.2	Usage Periods for the Public and Private Keys .....	47
<b>6.4</b>	<b><i>ACTIVATION DATA</i></b> .....	<b>47</b>
6.4.1	Activation Data Generation and Installation.....	47
6.4.2	Activation Data Protection.....	47
6.4.3	Other Aspects of Activation Data .....	47
<b>6.5</b>	<b><i>COMPUTER SECURITY CONTROLS</i></b> .....	<b>47</b>
6.5.1	Specific Computer Security Technical Requirements .....	47
6.5.2	Computer Security Rating.....	48
<b>6.6</b>	<b><i>LIFE-CYCLE TECHNICAL CONTROLS</i></b> .....	<b>48</b>
6.6.1	System Development Controls .....	48
6.6.2	Security Management Controls.....	49
6.6.3	Life Cycle Security Ratings .....	49
<b>6.7</b>	<b><i>NETWORK SECURITY CONTROLS</i></b> .....	<b>49</b>
<b>6.8</b>	<b><i>CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS</i></b> .....	<b>49</b>
<b>7.</b>	<b><i>CERTIFICATE AND CRL PROFILES</i></b> .....	<b>50</b>
<b>7.1</b>	<b><i>CERTIFICATE PROFILE</i></b> .....	<b>50</b>
7.1.1	Version Numbers .....	50
7.1.2	Certificate Extensions .....	50
7.1.3	Algorithm Object Identifiers .....	50
7.1.4	Name Forms .....	51

---

7.1.5	Name Constraints .....	51
7.1.6	Certificate Policy Object Identifier .....	51
7.1.7	Usage of Policy Constraints Extension.....	51
7.1.8	Policy Qualifiers Syntax and Semantics .....	51
7.1.9	Processing Semantics for the Critical Certificate Policy Extension.....	51
<b>7.2</b>	<b><i>CRL PROFILE</i></b> .....	<b>51</b>
7.2.1	Version Numbers .....	51
7.2.2	CRL Entry Extensions .....	51
<b>8.</b>	<b>SPECIFICATION ADMINISTRATION .....</b>	<b>52</b>
8.1	<b><i>SPECIFICATION CHANGE PROCEDURES</i></b> .....	<b>52</b>
8.2	<b><i>PUBLICATION AND NOTIFICATION POLICIES</i></b> .....	<b>52</b>
8.3	<b><i>CPS APPROVAL PROCEDURES</i></b> .....	<b>52</b>
<b>9.</b>	<b>BIBLIOGRAPHY .....</b>	<b>54</b>
<b>10.</b>	<b>ACRONYMS AND ABBREVIATIONS .....</b>	<b>56</b>
<b>11.</b>	<b>GLOSSARY.....</b>	<b>58</b>
<b>12.</b>	<b>ACKNOWLEDGEMENTS .....</b>	<b>70</b>

## DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
0.1	14 Jan 2001	Entrust	First Draft	Rough draft based on FBCA
0.2	13 Feb 2001	Entrust	Second Draft	Changes made USDA/NFC to USDA/NFC CA
0.3	23 Mar 2001	Entrust	Third Draft	Changes based on feedback from USDA/NFC
0.4	2 Aug 2001	Entrust	Fourth Draft	Changes based on feedback from USDA/NFC
0.5	19 Sept 01	NFC	Fifth Draft	Changes based on feedback from NFC staff
0.6	7 Dec 01	NFC	Sixth Draft	Changes based on NFC review
0.7	13 Dec 01	NFC	Seventh Draft	Changes based on NFC review
0.8	11 Jan 02	NFC	Eighth Draft	Changes based on discussions with consultants
0.9	21 Jan 02	NFC	Ninth Draft	Review by USDA/NFC personnel
1.0	6 Feb 02	NFC	Tenth Draft	Changes based on discussions with consultants
1.1	21 Mar 02	NFC	Eleventh Draft	Changes based on compliance audit



## **1. INTRODUCTION**

This Certificate Policy (CP) defines three certificate policies for use by the United States Department of Agriculture (USDA) / National Finance Center (NFC). The three policies represent three different assurance levels (Basic, Medium, and High) for public key digital certificates. The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber, performs its task.

The USDA/NFC Certification Authority (CA) serves as a CA for Federal Government Agencies and their business related entities. Those agencies, and their business related entities, desiring to have their employees conduct electronic transactions in a trusted manner, can do so by entering into a Memorandum of Agreement (MOA) with the USDA/NFC CA through its headquarters office (USDA/OCFO). Once the MOA is in place, participating agencies, known as Subscriber Organizations, designate a Local Registration Authority (LRA). The LRA’s perform the necessary verification procedures for the Subscriber Organization’s employees, known as Subscribers, who will actually receive certificates.

Any use of or reference to this CP outside the purview of the USDA/NFC PKI Policy Authority is completely at the using party’s risk. This USDA/NFC CA CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

The terms and provisions of this USDA/NFC CA CP shall be interpreted under and governed by applicable Federal law. The United States Government disclaims any liability that may arise from the use of this USDA/NFC CA CP.

### **1.1 OVERVIEW**

#### **1.1.1 Certificate Policy (CP)**

When a Certification Authority (CA) issues a certificate, it provides a statement to a certificate user that a particular public key is bound to a particular Entity. Different assurance level certificates may be issued and may be suitable for different applications and/or purposes.

Because of the importance of a Certificate Policy (CP) in establishing trust in a public key certificate, it is fundamental that the CP be understood and consulted by any Relying Party.

USDA/NFC CA certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OID (in this case, the USDA/National Finance Center) also publishes its CP for examination by Relying Parties.

### **1.1.2 Relationship Between the USDA/NFC CA CP and the USDA/NFC CA CPS**

The USDA/NFC CA CP states what assurance can be placed in a certificate issued by the USDA/NFC CA. The USDA/NFC CA CPS states how the USDA/NFC CA establishes that assurance.

## **1.2 IDENTIFICATION**

There are three levels of assurance in this Certificate Policy, which are defined in subsequent sections. Each level of assurance has an Object Identifier (OID) to be inserted into certificates issued by the USDA/NFC CA. The OID's are registered under the id-infosec arc as follows:

csor-certpolicy OBJECT IDENTIFIER	::= {2 16 840 1 101 3 2 1}
USDA-NFC-policies OBJECT IDENTIFIER	::= {csor-certpolicy 8}
id-usda-nfc-pki-certpcy-basicAssurance	::= USDA/NFC-policies 1
id- usda-nfc-pki-certpcy-mediumAssurance	::= USDA/NFC-policies 2
Id- usda-nfc-pki-certpcy-highAssurance	::= USDA/NFC-policies 3

## **1.3 COMMUNITY AND APPLICABILITY**

The following are roles relevant to the administration and operation of the USDA/NFC CA.

### **1.3.1 PKI Authorities**

#### **1.3.1.1 USDA/NFC Public Key Infrastructure Approval Authority**

This CP is established under the authority of and with the approval of the USDA/NFC Director and the concurrence of the associate CIO for Cyber Security.

#### **1.3.1.2 USDA/NFC PKI Policy Authority**

The USDA/NFC PKI Policy Authority is a committee established pursuant to the USDA/NFC Director. The USDA/NFC PKI Policy Authority is responsible for:

- ? The United States Department of Agriculture (USDA) National Finance Center (NFC) Certificate Policy (CP);
- ? Approving the USDA/NFC CA Certification Practice Statement (CPS);
- ? Accepting and revoking applications from Agencies desiring to use the USDA/NFC CA;

- ? Approving the policy mappings between certificates issued by the applicant Agency and the levels of assurance set forth in the USDA/NFC CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the USDA/NFC PKI Policy Authority); and

?

The USDA/OCFO will enter into a Memorandum of Agreement (MOA) with an Agency setting forth the respective responsibilities and obligations of both parties. The USDA/NFC Financial Management Office administers all of its MOA's. Thus, the term "MOA" as used in this CP shall always refer to the MOA cited in this paragraph.

#### **1.3.1.3 USDA/NFC CA Operational Authority**

The USDA/NFC CA OA is the organization that operates the USDA/NFC CA, including developing and maintaining the CPS, issuing USDA/NFC CA certificates when directed by the USDA/NFC PKI Policy Authority, posting those certificates and Certification Revocation Lists (CRLs) into the USDA/NFC CA repository, and ensuring the continued availability of the repository to all users.

After an Agency is authorized to use the USDA/NFC CA, ensuring continued conformance of that Agency with applicable requirements as a condition for allowing continued use of the USDA/NFC CA.

#### **1.3.1.4 USDA/NFC CA Operational Authority Administrator**

The Administrator is the individual within the USDA/NFC CA OA who has principal responsibility for overseeing the proper operation of the USDA/NFC CA including the USDA/NFC CA repository, and who oversees individuals in the positions of USDA/NFC CA OA Officers.

#### **1.3.1.5 USDA/NFC CA Operational Authority Officers**

These officers are the individuals within the USDA/NFC CA OA who operate the USDA/NFC CA and its repository. The roles include USDA/NFC CA OA Officer, Auditor, and Operator, all described in this and later sections of this CP.

#### **1.3.1.6 USDA/NFC CA Certification Authority (USDA/NFC CA)**

The USDA/NFC CA is the entity operated by the USDA/NFC CA OA that is authorized by the USDA PKI Policy Authority to create, sign, and issue public key certificates. As operated by the USDA/NFC CA OA, the USDA/NFC CA is responsible for all aspects of the issuance and management of a certificate including:

- ?? Control over the registration process,
- ?? Identification and authentication process,
- ?? Certificate manufacturing process,
- ?? Publication of certificates,

- ?? Revocation of certificates,
- ?? Re-key of USDA/NFC CA signing material, and
- ?? Ensuring that all aspects of the USDA/NFC CA services and USDA/NFC CA operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

#### **1.3.1.7 Registration Authority (RA and LRA)**

The Registration Authority (RA) and Local Registration Authority (LRA) are the entities that collect and verify each Subscriber's identity and information that are to be entered into his or her public key certificate. The USDA/NFC CA OA acts as the RA for the USDA/NFC CA, and performs its function in accordance with a CPS approved by the USDA/NFC PKI Policy Authority. The requirements for RA and LRA in USDA/NFC PKI are set forth in the sections below.

#### **1.3.1.8 Trusted Agents**

Trusted Agents act as an LRA in foreign locations and remote agency sites, if needed. The Trusted Agent will have the same responsibilities as the LRA in verifying basic and medium certificates. All Trusted Agents must sign an LRA agreement.

### **1.3.2 Related Authorities**

The USDA/NFC CA's operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The USDA/NFC CA CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

### **1.3.3 End Entities**

#### **1.3.3.1 Subscribers**

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. USDA/NFC CA Subscribers include appropriate USDA personnel, contracting government agency (known as Subscriber Organization) personnel, non-government contracting personnel, and possibly certain network or hardware devices.

#### **1.3.3.2 Relying Party**

A Relying Party is any entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

### 1.3.4 Applicability

The sensitivity of the information processed or protected using certificates issued by USDA/NFC CA will vary significantly. A Relying Party must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements at three increasing, qualitative levels of assurance: Basic, Medium and High. It is assumed that the USDA/NFC CA will issue at least one High assurance certificate, so the USDA/NFC CA will be operated at that level. The USDA/NFC CA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

The certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance Level	Applicability
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
High	This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

#### 1.3.4.1 Factors in Determining Usage

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the USDA/NFC PKI Policy Authority or the USDA/NFC CA OA. Nonetheless, this CP contains some helpful guidance, set forth below, which Relying Parties may consider in making their decisions. Further, Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget (OMB) implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as NIST Special Publication 800-25 covering the technical elements of using digital signatures).

## **1.4 CONTACT DETAILS**

The contact details for this CP and PKI are:

USDA/NFC PKI Operational Authority: Kathy Sharp, Chairperson

Title: Senior Computer Specialist  
Department: ISPCS/ISSO  
USDA/NFC  
Address: Post Office Box 60,000  
City, State: New Orleans, LA  
Zip Code: 70160

Tel: 1-504-255-5638  
Fax: 1-504-255-4131  
Email: kathy.sharp@usda.gov

USDA/NFC PKI Policy Authority: Theresa Trentacoste, Chairperson

Title: Supervisory Program Analyst  
Department: FSD/DAB  
USDA/NFC  
Address: Post Office Box 60,000  
City, State: New Orleans, LA  
Zip Code: 70160

Tel: 1-504-255-5324  
Fax: 1-504-255-4367  
Email: theresa.trentacoste@usda.gov



## **2. GENERAL PROVISIONS**

### **2.1 OBLIGATIONS**

The obligations described below pertain to the USDA/NFC CA (and, by implication, the USDA/NFC CA OA), and to the Subscriber Organization, which interacts with the USDA/NFC CA. The obligations applying to the Subscriber Organization pertain to their activities in assisting in the issuance of USDA/NFC CA certificates. Thus, where the obligations include, for example, a review (or audit) of the Subscriber Organization's operation, the purpose of that review pertains to compliance with this CP, its corresponding CPS, and any MOA in existence between that agency and the USDA/NFC CA.

#### **2.1.1 CA Obligations**

When issuing certificates through a Subscriber Organization to its Subscribers, the USDA/NFC CA shall comply with this CP, its corresponding CPS, and any MOA in existence between that agency and the USDA/NFC CA.

The USDA/NFC CA shall provide CA services 7-days per week, 24-hours per day, on a best effort basis or provide advance notification of any required downtime, with allowances for reasonable maintenance schedules, in accordance with the policies and processes described in the CPS. It shall issue certificates to Subscribers, in accordance with the certificate policies referenced in section 1.2 of the CPS as well as other procedures and practices described in this CPS. It shall revoke a certificate upon a valid request made to the business unit manager who performs the LRA responsibility. Revocation is to be in accordance with the stipulations of the relevant CP as well as those in section 4.4 of the USDA/NFC PKI CA CPS. It shall issue and publish CRLs on a regular schedule as per section 4.4 of the CPS. It shall notify End-Entities that certificates have been issued or that digital signature verification certificates have been revoked by providing access to certificate information and CRLs in the USDA/NFC CA repository. It shall notify others (e.g. Relying Parties) of certificate issuance/revocation by providing access to certificate information and CRLs in the USDA/NFC CA repository. It shall comply with all requirements set forth in Subscriber Organization MOAs.

#### **2.1.2 RA or LRA Obligations**

An RA or LRA who performs registration functions in support of a USDA/NFC CA described in 2.1.1 shall also comply with the requirements set forth in the MOA, and shall also be in compliance with USDA/NFC CA CP requirements.

#### **2.1.3 Subscriber Obligations**

Subscribers who receive certificates from USDA/NFC CA shall also be required to comply with the requirements set forth in their Subscriber Organization's MOA, along with compliance with this CP.

#### **2.1.4 Subscriber Organization Obligations**

The USDA/NFC CA CP, along with the Subscriber Organization MOA, specifies what steps are needed to perform the trust path creation, validation, and policy mappings in order for End Entities to rely upon a certificate.

#### **2.1.5 Repository Obligations**

The USDA/NFC CA OA may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- ?? X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol,
- ?? Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- ?? Access control mechanisms when needed to protect repository information as described in later sections.

#### **2.1.6 Certificate Issuance to Non-US Government Parties**

The USDA/NFC CA may issue certificates to parties other than agencies, officers and employees of the U.S. Government, such as contractors and parties affiliated with USDA/NFC CA agencies, for the convenience of the U.S. Government when those parties have a bona fide need to possess a certificate issued by the USDA/NFC CA, as established by the USDA/NFC PKI Policy Authority. In each such case, an MOA or similar instrument shall be executed, and shall contain whatever provisions are determined appropriate by the USDA/NFC PKI Policy Authority.

### **2.2 LIABILITY**

The United States Government disclaims any liability that may arise from use of any certificate issued by the USDA/NFC CA, or the USDA/NFC PKI Policy Authority's determination to revoke a certificate issued by the USDA/NFC CA. In no event will the U.S. Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the USDA/NFC CA.

### **2.3 FINANCIAL RESPONSIBILITY**

This CP contains no limits on the use of any certificates, issued by the USDA/NFC CA. Instead, Relying Parties shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction. Thus, one Relying Party may be willing to accept a Basic assurance level certificate for transactions of a financial value for which another Relying Party would require a High assurance level certificate. This is entirely at the discretion of the Relying Party and is likely to depend upon several factors in addition to the certificate assurance level (e.g., likelihood of fraud, other procedural controls, Relying Party specific policy or statutorily imposed constraints).

#### **2.3.1 Indemnification by Relying Parties and Subscribers**

No stipulation.

### **2.3.2 Fiduciary Relationships**

Issuance of certificates by the USDA/NFC CA and assistance in that issuance by a USDA/NFC RA or LRA does not make the USDA/NFC CA, RA, or LRA an agent, fiduciary trustee, or other representative of any authorized Subscribers or Relying Parties.

### **2.3.3 Administrative Processes**

Administrative processes pertaining to this CP shall be determined by the USDA/NFC CA OA pursuant to the agreement between it and the USDA/NFC PKI Policy Authority for the operation of the USDA/NFC CA.

## **2.4 INTERPRETATION AND ENFORCEMENT**

### **2.4.1 Agency Policy**

The USDA/NFC CA shall be subject to all agency policies that apply to employee use and misuse of computer systems.

### **2.4.2 Governing Law**

All applicable Federal laws and regulations shall govern the enforceability, construction, interpretation, and validity of this CP and CPS.

### **2.4.3 Severability of Provisions, Survival, Merger, and Notice**

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. Severance or merger of entities may result in changes of the scope, management, and/or operations of this PKI and may require updates to this CP. The process for updating this CP is described in section 8.1.

### **2.4.4 Dispute Resolution Procedures**

The USDA/NFC PKI OA shall resolve any disputes associated with the use of the USDA/NFC CA or certificates issued by the USDA/NFC CA. Any party not satisfied by the OA's resolution may appeal to the USDA OGC for final arbitration.

## **2.5 FEES**

The USDA/NFC CA is part of the USDA/NFC working capital fund. As such, the USDA/NFC CA OA shall charge a fee, which shall include appropriate overhead, to each Subscriber Organization in order to fund the operation of the USDA/NFC CA.

## **2.6 PUBLICATION AND REPOSITORY**

### **2.6.1 Publication of CA Information**

The USDA/NFC CA PA shall publish all information concerning the USDA/NFC CA necessary to support its use and operation. That information includes, but is not limited to, this CP, its related forms and other documents necessary for a potential user of the USDA/NFC CA services to be able to make an informed decision about such services.

Other documents, such as the CPS, certificate and directory information, may be made available under a non-disclosure agreement, at the discretion of the USDA/NFC PA.

### **2.6.2 Frequency of Publication**

USDA/NFC CA certificates and certificate status information shall be published as specified in this CP.

### **2.6.3 Access Controls**

The USDA/NFC CA OA shall protect any repository information not intended for public dissemination or modification. Certificates and CRL's shall be available to Subscribers and Relying Parties from the USDA/NFC CA repository, which is read-only.

### **2.6.4 Repositories**

The protocol used to access the USDA/NFC CA repository shall be the Lightweight Directory Access Protocol (LDAP) Version 3.

## **2.7 COMPLIANCE AUDIT**

The USDA/NFC CA shall have a compliance audit mechanism in place. This mechanism shall ensure that the requirements of the CP and CPS and the provisions of any Subscriber Organization's MOA are being implemented and enforced.

### **2.7.1 Frequency of Entity Compliance Audit**

The USDA/NFC CA, RA's and LRA's shall be subject to a periodic compliance audit no less frequent than once per year for High and Medium Assurance, and no less than once every two years for Basic Assurance.

The USDA/NFC CA shall have the right to require periodic and aperiodic compliance audits or inspections LRA operations to validate that their Subscriber Organization is operating in accordance with the requirements of this CP, CPS and Agency MOA. Further, the USDA/NFC PKI Policy Authority shall have the right to require aperiodic compliance audits of CA's that interoperate with the USDA/NFC CA under this CP. The USDA/NFC PKI Policy Authority shall state the reason for any aperiodic compliance audit.

### **2.7.2 Identity/Qualifications of Compliance Auditor**

The auditor shall demonstrate competence in the field of compliance audits, and be thoroughly familiar with requirements which the USDA/NFC PKI Policy Authority imposes on the issuance and management of USDA/NFC CA certificates. The compliance auditor shall perform such compliance audits as a primary responsibility. The USDA/NFC CA OA shall identify the compliance auditor for the USDA/NFC CA, with the concurrence of the Designated Approving Authority (DAA).

### **2.7.3 Compliance Auditor's Relationship to Audited Party**

The USDA/NFC CA's compliance auditor either shall be a private firm that is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. The USDA/NFC PKI Policy Authority shall determine whether a compliance auditor meets this requirement.

### **2.7.4 Topics Covered by Compliance Audit**

The purpose of a compliance audit shall be to verify that all entities subject to this CP comply with the requirements of this CP, the CPS, the signed MOA, and any and all signed forms, as applicable.

### **2.7.5 Actions Taken as a Result of Deficiency**

The USDA/NFC PKI Policy Authority determines whether the USDA/NFC CA is complying with its obligations as set forth in this CP. As such, the USDA/NFC PKI Policy Authority may suspend operation of the USDA/NFC CA if there is a compliance deficiency of a serious nature, or it may direct that other corrective actions be taken which allow interoperation to continue. The USDA/NFC PKI Policy Authority will develop procedures for this purpose.

When the compliance auditor finds a discrepancy between how the USDA/NFC CA is designed or is being operated or maintained and the requirements of this CP, the following actions shall be performed:

- ?? The compliance auditor shall note the discrepancy;
- ?? The compliance auditor shall notify any relevant entities in accordance with established MOAs or cross-certifying agreements in the event of a severe discrepancy;
- ?? The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the USDA/NFC PKI Policy Authority may decide to temporarily halt operation of the USDA/NFC CA, to revoke a certificate issued by the USDA/NFC CA, or take other actions it deems appropriate. The USDA/NFC PKI Policy Authority shall develop procedures for making and implementing such determinations.

### **2.7.6 Communication of Result**

An Audit Compliance Report, including identification of corrective measures taken or being taken by the auditee, shall be provided to the USDA/NFC PKI Policy Authority as set forth in section 2.7.1. Additionally, where necessary, the results shall be communicated as set forth in 2.7.5 above.

## **2.8 CONFIDENTIALITY**

USDA/NFC CA shall release information in accordance with 5 U.S.C. 552, Freedom of Information Act, as amended. For specific information on accessing records, administrative processes, fees and fee waivers, and exemptions, interested parties should refer directly to the FOIA and its regulations. USDA/NFC CA shall include FOIA provisions in any MOA it enters into with a Subscriber Organization.

## **2.9 INTELLECTUAL PROPERTY RIGHTS**

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this CP.

### **3. IDENTIFICATION AND AUTHENTICATION**

#### **3.1 INITIAL REGISTRATION**

##### **3.1.1 Types of Names**

The USDA/NFC CA shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN); the X.500 DN may also contain domain component elements. Certificates issued to the RA's shall use the DN form, and have an assurance level equal to, or greater than, the highest level of assurance of the certificates the CA issues to subscribers or other CA's. Where DN's are required, subscribers shall have them assigned through their organizations, in accordance with USDA/NFC PKI standards as described in 3.1.1 of the CPS, and furnished to all agencies having a signed MOA in place. Certificates may additionally assert an alternate name form subject to requirements set forth below intended to ensure name uniqueness. The table below describes the naming requirements that apply to each level of assurance.

Basic	Non-Null Subject Name, and optional Alternative Subject Name if marked non-critical
Medium	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical
High	X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical

##### **3.1.2 Need for Names to be Meaningful**

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates shall identify the person or object to which they are assigned in a meaningful way.

When DN's are used, it is preferable that the common name represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter). However, at the Basic assurance levels, a DN for human subscribers may also be a pseudonym (such as a large number) as long as it respects name space uniqueness requirements.

##### **3.1.3 Rules for Interpreting Various Name Forms**

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the USDA/NFC PKI Policy Authority.

### **3.1.4 Uniqueness of Names**

Name uniqueness across the USDA/NFC PKI shall be enforced. The USDA/NFC CA's and RA's shall enforce name uniqueness within the X.500 name space for which they have been authorized. When other name forms are used, they too shall be allocated such that name uniqueness across the USDA/NFC PKI is ensured.

The USDA/NFC CA's shall document in the CPS:

- ?? What name forms shall be used,
- ?? How the USDA/NFC CA's and RA's will interact with the USDA/NFC PKI Policy Authority to ensure this is accomplished, and
- ?? How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names?).

### **3.1.5 Name Claim Dispute Resolution Procedure**

The USDA/NFC PKI Policy Authority shall resolve any name collisions brought to its attention that may affect interoperability using the USDA/NFC CA.

### **3.1.6 Recognition, Authentication and Role of Trademarks**

No stipulation.

### **3.1.7 Method to Prove Possession of Private Key**

Where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the USDA/NFC CA. The USDA/NFC CA then validates the signature using the party's public key. The USDA/NFC PKI Policy Authority may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated directly on the party's token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer. If the party is not in possession of the token when the key is generated, then the token shall be delivered to the subject via an accountable method (see Section 6.1.2).

For all assurance levels, when keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The USDA/NFC CA shall maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the USDA/NFC CA's are the only recipients of this shared secret.

### 3.1.8 Authentication of Organizational Identity

Requests for USDA/NFC CA certificates in the name of an organization shall include the organizational name, address, and documentation of the existence of the entity. The USDA/NFC CA OA RA and LRA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the entity. Authentication for issuance of cross-certificates to another CA will be processed through the FBCA or directly with the USDA/NFC CA, in accordance with this CP and CPS.

### 3.1.9 Authentication of Individual Identity

For Subscribers, the USDA/NFC CA's shall ensure that the applicant's identity information is verified and checked in accordance with the applicable CP and CPS. The USDA/NFC CA's, RA's and LRA's shall ensure that the applicant's identity information and public key are properly bound. Additionally, the USDA/NFC CA's, RA's and LRA's shall record the process that was followed for issuance of each certificate.

Process information shall depend upon the certificate level of assurance and shall be addressed in the USDA/NFC PKI CA CPS. The process documentation and authentication requirements shall include the following depending on the level of assurance (as set forth below):

- ?? The identity of the person performing the identification
- ?? A signed declaration by that person that he or she verified the identity of the Subscriber as required by the certificate policy which may be met by establishing how the applicant is known to the verifier;
- ?? A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant;
- ?? The date and time of the verification; and
- ?? A declaration of identity signed by the applicant using a handwritten signature. If in-person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication.

The table below summarizes the identification requirements for each level of assurance.

Assurance Level	Identification Requirements
Basic	Identity shall be established by in-person proofing before the Registration Authority, LRA, Trusted Agent or an entity certified by a State or Federal Agency as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the applicant and the applicant's management may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or one Non-Federal Government I.D.s, (e.g., Drivers License).
Medium	Identity shall be established by in-person proofing before the Registration Authority, LRA, Trusted Agent or an entity certified by a State or Federal Agency as being authorized to confirm identities;

	information provided shall be verified to ensure legitimacy. Credentials required are one Federal Government-issued Picture I.D. and one Non-Federal Government photo I.D. (e.g., Drivers License)
High	Identity established by in-person appearance before the Registration Authority or LRA; information provided shall be checked to ensure legitimacy. Credentials required are one Federal Government-issued Picture I.D. and one Non-Federal Government photo I.D. (e.g., Drivers License)

The documentation and authentication process requirements are accomplished by the completion of an NFC Certificate Action Request Form in accordance with the instructions. A Subscriber Agreement, signed by the applicant using a handwritten signature in the presence of the person performing the identity authentication, is submitted along with all required documentation attached (e.g. copy of photo Ids, Certificate Action Request Form, etc.). All of the above stated forms are available at <http://www.usda.nfc.gov/>.

**For All Assurance Levels:** If an Applicant is unable to perform face-to-face registration alone (e.g., a network device), the applicant shall be represented by a trusted person already issued a digital certificate by the USDA/NFC CA. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

### 3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects, in which case the component shall have a human sponsor, who is responsible for providing the following information:

- ?? Equipment identification
- ?? Equipment public keys
- ?? Equipment authorizations and attributes (if they are to be included in the certificate)
- ?? Contact information to enable the CA or LRA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested, with in person registration by the sponsor and the identity of the sponsor confirmed in accordance with the requirements of Section 3.1.9.

## 3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

### 3.2.1 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtain new keys. As long as Subscriber's Certificate has not been revoked prior to the end of the expiration of the current key

pair, a request may be made for the issuance of a new certificate with a new key pair. The CA may initiate this process or the subscriber shall make such a request by completing and signing a Certificate Action Request Form. Once the form is received by the LRA, the LRA then performs the update, upgrade, revocation or other certificate modification as necessary. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. Authentication of the Subscriber's identity as defined in section 3.1.9 of the CPS shall be in accordance with the following table:

Assurance Level	Routine Rekey Identity Requirements for Subscriber Signature and Encryption Certificates
Basic	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration
Medium	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration

### 3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRL's. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. Thus, a CA may choose to create a certificate good for one year, renew it twice (each for a one-year period), and then re-key at the end of the third year. The USDA/NFC CA shall not renew a certificate without performing a re-key.

### 3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields from the old certificate. For example, a CA may choose to update a certificate of a Subscriber whose characteristics have

changed (e.g., has just received a medical degree). The old certificate may or may not be revoked, but shall not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change shall be provided to the RA, LRA or other designated agent (as set forth above) in order for an updated certificate having the new name to be issued.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all RAs, LRA's and subscribers that rely on the CA's certificate that it has been changed. For self-signed ("root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

### ***3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION***

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1 above.

### ***3.4 REVOCATION REQUEST***

Revocation requests shall be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

## **4. OPERATIONAL REQUIREMENTS**

### **4.1 APPLICATION FOR A CERTIFICATE**

The USDA/NFC PKI Operational Authority will evaluate certificate applications in accordance with procedures of this CP and CPS and make a determination regarding whether or not to issue the requested certificate(s). The USDA/NFC PKI Policy Authority and the applicant's Subscriber Organization will then enter into an MOA setting forth their respective responsibilities. An Applicant shall execute a Subscriber Agreement. Applicants will also complete a Certificate Request Form and provide the requested information to their LRA in a form prescribed by the USDA/NFC CA in accordance with this Policy. The USDA/NFC PKI Operational Authority will then direct the USDA/NFC CA RA to issue the certificate(s) in accordance with this CP and CPS.

#### **4.1.1 Delivery of Public Key for Certificate Issuance**

Public keys shall be delivered for certificate issuance in a way that binds the applicant's verified identification to the public key. For all levels of assurance, this binding may be accomplished using cryptography. If cryptography is used, it shall be at least as strong as that employed in certificate issuance. Additionally, this binding may also be accomplished using agreed upon non-cryptographic physical and procedural secured mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request.

In those cases where public/private key pairs are generated by the USDA/NFC CA on behalf of the Subscriber, the USDA/NFC CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The USDA/NFC CA shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

### **4.2 CERTIFICATE ISSUANCE**

Upon receiving a request for a certificate, the LRA shall respond in accordance with the requirements set forth in the CP and CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in the CP and CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the LRA to verify that the information is correct and accurate.

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. RA's will, at a minimum, perform a visual check of the certificate's DN prior to issuance.

If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

#### **4.2.1 Delivery of Subscriber's Private Key to Subscriber**

In most cases, a private key shall be generated and remain within the cryptographic boundary of the cryptographic module.

The USDA/NFC CA shall not issue a certificate to multiple users.

In the case of a roaming certificate, the USDA/NFC PKI shall only retain access to the encrypted Subscriber's private key. That key shall be maintained in a double encrypted state, with the first decryption key controlled by the Subscriber and only after that decryption, with a key controlled by the CA. The private signing key shall be downloaded in an encrypted format to the Subscriber for the duration of the authentication session. Decryption can only take place through the use of the subscriber's private key pass phrase. At the end of the authentication session all evidence of the subscriber's private signing key shall be removed. Under no circumstances shall anyone other than the Subscriber have knowledge of or control over private signing keys and anyone generating a private signing key for a Subscriber shall not retain any copy of that key. In non-roaming solutions, the private signing key shall be maintained in an encrypted format on the subscriber's desktop. Hardware tokens containing USDA/NFC CA private signature keys may be backed-up in accordance with security audit requirements defined in Section 4.5.1.

#### **4.2.2 USDA/NFC CA Public Key Delivery and Use**

The public key of the USDA/NFC CA shall be available for certification trust paths to be created and verified. That key will appear in the form of a certificate issued by the USDA/NFC CA. In order to extract that key from the certificate with confidence that it has not been altered, the USDA/NFC CA shall ensure that its Subscribers obtain its self-signed root certificate in a trustworthy fashion. Such a self-signed root certificate is sometimes called a Trusted Certificate. Acceptable methods for Trusted Certificate delivery include but are not limited to:

- ?? The CA loading a Trusted Certificate onto tokens delivered to Subscribers via secure mechanisms;
- ?? Secure distribution of Trusted Certificates through secure out-of-band mechanisms;
- ?? Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- ?? Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

### **4.3 CERTIFICATE ACCEPTANCE**

The USDA/NFC CA shall define in its forms and agreements with its subscribers what constitutes acceptance of a certificate. The process of issuance and acceptance shall be accomplished in a secure manner as described in the USDA/NFC CA CPS.

All Subscribers shall be required to sign a NFC Certificate Action Request Form and a Subscriber Agreement containing the requirements regarding private key protection and certificate use. The signing of the Subscriber Agreement constitutes certificate acceptance.

## **4.4 CERTIFICATE REVOCATION**

### **4.4.1 Circumstances for Revocation of a Certificate Issued by the USDA/NFC CA**

A certificate shall be revoked when the binding between the subject and the subject's public key contained within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include:

- ?? Identifying information in the certificate has become invalid;
- ?? The Subscriber or his Subscriber Organization can be shown to have violated, or is suspected of violating, the requirements of either the USDA/NFC CA CP or the respective MOA;
- ?? The private key has been or is suspected of having been compromised, or has been lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control over the use of the private key.

### **4.4.2 Who can Request Revocation of a Certificate Issued by the USDA/NFC CA**

A USDA/NFC CA certificate may be revoked upon direction of the USDA/NFC PKI Policy Authority or upon an authenticated request by a previously designated Subscribing Organization official. Such official or officials shall be identified in the MOA as authorized to make such a request.

The process for requesting revocation of a Subscriber certificate issued by the USDA/NFC CA shall be set forth in the CP or CPS. Revocation normally will proceed once:

- ?? A Subscriber Organization receives sufficient evidence of compromise or loss of any subscriber's corresponding private key,
- ?? An authenticated request is made to the Subscriber Organization by the holder of the private key, or
- ?? Someone in his or her supervisory chain, or an officially designated administrative or information security officer, makes an authenticated request for revocation.

A Subscriber may always request the revocation of his or her certificate through procedures described in Section 4.4.3. Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

### **4.4.3 Procedure for Revocation Request**

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. Revocation requests are accomplished by the completion and signing of an NFC Certificate Action Request Form in accordance with procedures set forth in this CP and CPS.

Upon receipt of a revocation request involving a USDA/NFC CA certificate, the USDA/NFC CA OA shall authenticate the request. The USDA/NFC PKI Policy Authority may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. The USDA/NFC PKI Policy Authority shall direct the USDA/NFC CA OA to revoke the certificate by placing its serial number and other identifying information on a CRL and then post the CRL in the USDA/NFC CA repository.

For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an Agency that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the Agency. If a Subscriber leaves an Agency and the hardware tokens cannot be obtained from the Subscriber, then all Subscribers' certificates associated with the unretrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed prior to, or immediately upon, surrender in the presence of the Subscriber..

#### **4.4.4 Revocation of a Certificate Issued by the USDA/NFC CA**

Revocation of a USDA/NFC CA certificate shall take effect upon the publication into the USDA/NFC CA repository of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment) that identifies the certificate as being revoked, within the time limits as specified in Section 4.4.9 (starting from the time the request is authenticated or sufficient evidence of compromise or loss is received). Further, and separate from the publication of the status information, prompt oral or electronic notification shall be given by the USDA/NFC CA OA. Information about a revoked certificate shall remain in the status information until the certificate expires and for one additional CRL beyond that point. A certificate may be removed from the second CRL issued after it expires.

#### **4.4.5 Revocation Request Grace Period**

There is no revocation grace period for the USDA/NFC CA. Grace periods for a Subscriber to submit a revocation request to the RA or LRA shall be set forth in the USDA/NFC CPS.

#### **4.4.6 Certification Authority Revocation Lists / Certificate Revocation Lists**

The USDA/NFC CA's shall issue Certificate Revocation Lists (CRL). To the extent practical, the contents of CRL's shall be checked before issuance to ensure that all information is correct. This may be done using software, which scans the CRL's looking for any evidence of an improperly manufactured CRL.

#### **4.4.7 CRL Issuance Frequency**

CRL's shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. The USDA/NFC CA shall ensure that superseded certificate status information is removed from the repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

The following table provides CRL issuance requirements.

<b>Assurance Level</b>	<b>CRL Issuance Frequency for CA's (Routine)</b>	<b>CRL Issuance for CA's (Loss or Compromise of Private Key)</b>
Basic	At Least Once Each Day	Within 24 Hours of Notification
Medium	At Least Once Each Day	Within 18 Hours of Notification
High	At Least Once Each Day	Within 6 Hours of Notification

#### **4.4.8 CRL Checking Requirements**

Use of revoked certificates could have damaging or catastrophic consequences. It is the responsibility of the Relying Party to determine how often new revocation data should be obtained, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

#### **4.4.9 On-line Revocation / Status Checking Availability**

In addition to CRL's, client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process /CRL's. The USDA/NFC PKI Policy Authority will determine when and under what circumstances the USDA/NFC CA OA will provide on-line status checking of USDA/NFC CA certificates.

#### **4.4.10 Other Forms of Revocation Advertisements Available**

No stipulation.

#### **4.4.11 Checking Requirements for Other Forms of Revocation Advertisements**

No stipulation.

#### **4.4.12 Special Requirements Related to Key Compromise**

In the event of a USDA/NFC CA private key compromise or loss, a CRL shall be immediately published revoking all certificates issued by the USDA/NFC CA. The USDA/NFC CA, if operating at the High Assurance level and using reason codes, shall have the ability to transition any reason code to key compromise.

### **4.5 SECURITY AUDIT PROCEDURE**

Audit log files shall be generated for all events relating to the security of the USDA/NFC CA's. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit

logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention Period for Archive*, Section 4.6.2.

#### 4.5.1 Types of Events Recorded

All security auditing capabilities of the USDA/NFC CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. (Note: the table below may be replaced in future releases of this CP with a reference to the Certificate Issuing and Management Components Protection Profile being developed by NIST.) Auditing capabilities relevant to Test Assurance level shall be set forth in the MOA and are not described below. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- ?? The type of event
- ?? The date and time the event occurred
- ?? A success or failure indicator when executing the USDA/NFC CA's signing process
- ?? A success or failure indicator when performing certificate revocation
- ?? The identity of the entity and/or operator (of the USDA/NFC CA) that caused the event.
- ?? A message from any source requesting an action by the USDA/NFC CA is an auditable event. The message shall include message date and time, source, destination and contents.

Auditable Event	Basic	Medium	High
<b>SECURITY AUDIT</b>			
Any changes to the Audit parameters e.g., audit frequency, type of event audited	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X
<b>IDENTIFICATION AND AUTHENTICATION</b>			
Successful and unsuccessful attempts to assume a role	X	X	X
Change in the value of maximum authentication attempts	X	X	X
Maximum number of unsuccessful authentication attempts during user login	X	X	X
An Administrator unlocks an account that has been	X	X	X

<b>Auditable Event</b>	<b>Basic</b>	<b>Medium</b>	<b>High</b>
locked as a result of unsuccessful authentication attempts			
An Administrator changes the type of authenticator e.g., from password to biometrics	X	X	X
<b>KEY GENERATION</b>			
Whenever the USDA/NFC CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X
<b>PRIVATE KEY LOAD AND STORAGE</b>			
The loading of Component private keys	X	X	X
All access to certificate subject private keys retained within the USDA/NFC CA for key recovery purposes	X	X	X
<b>TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE</b>			
All changes to the trusted public keys, including additions and deletions	X	X	X
<b>PRIVATE AND SECRET KEY EXPORT</b>			
The export of private keys (keys used for a single session or message are excluded)	X	X	X
<b>CERTIFICATE REGISTRATION</b>			
All certificate requests	X	X	X

<b>Auditable Event</b>	<b>Basic</b>	<b>Medium</b>	<b>High</b>
<b>CERTIFICATE REVOCATION</b>			
All certificate revocation requests	X	X	X
<b>CERTIFICATE STATUS CHANGE APPROVAL</b>			
The approval or rejection of a certificate status change request	X	X	X
<b>USDA/NFC CA CONFIGURATION</b>			
Any security-relevant changes to the configuration of the USDA/NFC CA	X	X	X
<b>ACCOUNT ADMINISTRATION</b>			
Roles and users are added or deleted	X	X	X
The access control privileges of a user account or a role are modified	X	X	X
<b>CERTIFICATE PROFILE MANAGEMENT</b>			
All changes to the certificate profile	X	X	X
<b>REVOCATION PROFILE MANAGEMENT</b>			
All changes to the revocation profile	X	X	X
<b>CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT</b>			
All changes to the certificate revocation list profile	X	X	X

Auditable Event	Basic	Medium	High
<b>MISCELLANEOUS</b>			
Installation of the Operating System	X	X	X
Installation of the USDA/NFC CA	X	X	X
Installing hardware cryptographic modules		X	X
Removing hardware cryptographic modules		X	X
Destruction of cryptographic modules	X	X	X
System Startup	X	X	X
Logon Attempts to USDA/NFC CA applications	X	X	X
Receipt of Hardware / Software		X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Backing up USDA/NFC CA internal database	X	X	X
Restoring USDA/NFC CA internal database	X	X	X
File manipulation (e.g., creation, renaming, moving)		X	X
Posting of any material to a repository		X	X
Access to USDA/NFC CA internal database		X	X
All certificate compromise notification requests	X	X	X
Loading tokens with certificates		X	X
Shipment of Tokens		X	X
Zeroizing tokens	X	X	X
Rekey of the USDA/NFC CA	X	X	X
Configuration changes to the CA server involving:			

<b>Auditable Event</b>	<b>Basic</b>	<b>Medium</b>	<b>High</b>
Hardware	X	X	X
Software	X	X	X
Operating System	X	X	X
Patches	X	X	X
Security Profiles		X	X
<b>PHYSICAL ACCESS / SITE SECURITY</b>			
Personnel Access to room housing USDA/NFC CA		X	X
Access to the USDA/NFC CA server		X	X
Known or suspected violations of physical security	X	X	X
<b>ANOMALIES</b>			
Software Error conditions	X	X	X
Software check integrity failures	X	X	X
Receipt of improper messages		X	X
Misrouted messages		X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	X	X
Electrical power outages		X	X
Uninterruptible Power Supply (UPS) failure		X	X
Obvious and significant network service or access failures		X	X
Violations of Certificate Policy	X	X	X

Auditable Event	Basic	Medium	High
Violations of Certification Practice Statement	X	X	X
Resetting Operating System clock	X	X	X

#### 4.5.2 Frequency of processing data

Audit logs shall be reviewed in accordance with the table below. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Assurance Level	Review Audit Log
Basic	Only required for cause
Medium	At least once every two months  Statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
High	At least once per month  Statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

For the USDA/NFC CA, a statistically significant sample of security audit data generated by the USDA/NFC CA since the last review shall be examined.

#### 4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described in Section 4.5.4 below. The individual who removes audit logs from the USDA/NFC CA system shall be an official different from the individual who, in combination, command the USDA/NFC CA signature key.

#### **4.5.4 Protection of Audit Log**

The audit process shall not be done by or under the control of the USDA/NFC CA OA. A system configuration and procedures shall be implemented together to ensure that:

- ?? only authorized people have read access to the logs;
- ?? only authorized people may archive or delete audit logs; and
- ?? audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures shall be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the USDA/NFC CA equipment.

#### **4.5.5 Security Audit Data Backup Procedures**

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

#### **4.5.6 Security Audit Collection System (Internal vs. External)**

The audit log collection system may or may not be external to the USDA/NFC CA system. Audit processes shall be invoked at system startup and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the USDA/NFC CA OA Administrator shall determine whether to suspend the USDA/NFC CA operation until the problem is remedied.

#### **4.5.7 Notification to Event-causing Subject**

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

#### **4.5.8 Vulnerability Assessments**

Routine self-assessment of security controls shall be performed by the entity operating the CA.

### **4.6 RECORDS ARCHIVAL**

#### **4.6.1 Types of Events Archived**

USDA/NFC CA archive records shall be sufficiently detailed to establish the proper operation of the USDA/NFC CA, or the validity of any certificate (including those revoked or expired) issued by the USDA/NFC CA.

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

<b>Data To Be Archived</b>	<b>Basic</b>	<b>Medium</b>	<b>High</b>
USDA/NFC CA accreditation (if applicable)	X	X	X
Certification Practice Statement	X	X	X
Contractual obligations	X	X	X
System and equipment configuration	X	X	X
Modifications and updates to system or configuration	X	X	X
Certificate requests	X	X	X
Revocation requests	X	X	X
Subscriber identity Authentication data as per Section 3.1.9	X	X	X
Documentation of receipt and acceptance of certificates	X	X	X
Documentation of receipt of tokens	X	X	X
All certificates issued or published	X	X	X
Record of USDA/NFC CA Re-key	X	X	X
All CRL's issued and/or published	X	X	X
All Audit Logs	X	X	X
Other data or applications to verify archive contents	X	X	X
Documentation required by compliance auditors	X	X	X

#### **4.6.2 Retention Period for Archive**

The USDA/NFC PKI CA shall retain CA records for the minimum retention periods as identified below. The minimum retention periods are subject to change depending on the outcome of pending legal guidance.

This minimum retention period for these records is intended only to facilitate the operation of the USDA/NFC CA's.

Assurance Level	Minimum Retention Period
Basic	7 Years & 6 Months
Medium	10 Years & 6 Months
High	20 Years & 6 Months

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for a period determined by the USDA/NFC PKI Policy Authority for the USDA/NFC CA.

Prior to the end of the archive retention period, the USDA/NFC CA shall provide archived data and the applications necessary to read the archives to a USDA/NFC PKI Policy Authority approved archival facility, which shall retain the applications necessary to read this archived data.

#### **4.6.3 Protection of Archive**

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the USDA/NFC CA, archived records may be moved to another medium when authorized by the USDA/NFC CA OA Administrator. The contents of the archive shall not be released except as determined by the USDA/NFC PKI Policy Authority for the USDA/NFC CA or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the USDA/NFC CA itself.

#### **4.6.4 Archive Backup and Management**

The USDA/NFC CA shall perform scheduled, automated backups on a daily basis with mechanisms for off-site storage and retrieval.

#### **4.6.5 Requirements for Time-stamping of Records**

All backup software used for the purposes of section 4.6.4 shall maintain the backup media in a format affording chronological retrieval capabilities.

#### **4.6.6 Procedures to Obtain and Verify Archive Information**

Procedures detailing how to create, verify, package, transmit, and store the USDA/NFC CA archive information shall be published in the USDA/NFC CA CPS.

### **4.7 KEY CHANGE OVER**

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid certificate will be available to verify old signatures until all of the certificates

signed using the associated private key have also expired. If the old private key is used to sign CRL's that contain certificates signed with that key, then the old key shall be retained and protected.

The USDA/NFC's signing key shall have a validity period of half the lifetime of the corresponding certificate. The certificate lifetime will be not more than 10 years.

## **4.8 COMPROMISE AND DISASTER RECOVERY**

### **4.8.1 Computing Resources, Software, and/or Data are Corrupted**

If USDA/NFC CA equipment is damaged or rendered inoperative, but the USDA/NFC CA signature keys are not destroyed, USDA/NFC CA operation shall be re-established as quickly as possible, giving priority to the ability to generate certificate status information.

### **4.8.2 USDA/NFC CA Signature Keys are Revoked**

If the USDA/NFC CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then the USDA/NFC PKI Policy Authority and all of its Subscriber Organizations shall be immediately and securely notified in a fashion set forth in the MOA. This will allow Relying Parties to protect their interests. . The USDA/NFC PKI Policy Authority shall determine whether to revoke the USDA/NFC CA certificate. The USDA/NFC CA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. The USDA/NFC CA shall immediately and securely advise the USDA/NFC PKI Policy Authority and all of its Subscriber Organizations in the event of a disaster where the USDA/NFC CA installation is physically damaged and all copies of the USDA/NFC CA signature keys are destroyed.

### **4.8.3 USDA/NFC CA Signature Keys are Compromised**

If the USDA/NFC CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- ?? The USDA/NFC CA and all of its Subscriber Organizations shall be immediately and securely notified (so that agencies may issue CRLs revoking any certificates issued by the USDA/NFC CA);
- ?? The USDA/NFC CA shall immediately publish a CRL revoking the USDA/NFC CA's issued certificate as set forth above;
- ?? A new USDA/NFC CA key pair shall be generated by the USDA/NFC CA in accordance with procedures set forth in the USDA/NFC CPS; and
- ?? New USDA/NFC CA certificates shall be issued to Subscriber Organization' Subscribers in accordance with the USDA/NFC CPS.

The USDA/NFC CA governing body shall also investigate and report to the USDA/NFC PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

#### **4.8.4 Secure Facility Impaired After a Natural or Other type of Disaster**

In the case of a disaster whereby the USDA/NFC CA installation is physically damaged and all copies of the USDA/NFC CA signature key are destroyed as a result, the USDA/NFC PKI Policy Authority and all of its Subscriber Organizations shall be immediately and securely notified, and the USDA/NFC PKI Policy Authority shall take whatever action it deems appropriate.

The USDA/NFC CA installation shall be deployed so as to provide 24 hour, 365 days per year availability as per Section 5.1 of this CP. Backup will be performed in accordance with the USDA/NFC's Disaster Recovery Plan. The USDA/NFC PKI OA shall implement features to provide high levels of reliability.

Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending re-establishment of USDA/NFC CA operation with new certificates.

### **4.9 CA TERMINATION**

In the event of termination of the USDA/NFC CA operation, certificates signed by the USDA/NFC CA shall be revoked and the USDA/NFC PKI Policy Authority shall advise Subscriber Organizations with MOA's that USDA/NFC CA operations have terminated. Prior to USDA/NFC CA termination, the USDA/NFC CA shall provide archived data to the USDA/NFC PKI Policy Authority approved archival facility.

Subscriber Organizations will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the USDA/NFC CA is terminated.

## **5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS**

### **5.1 PHYSICAL CONTROLS FOR THE USDA/NFC CA OR AGENCY CA**

The USDA/NFC CA shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the USDA/NFC CA.

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

#### **5.1.1 Site Location and Construction**

The location and construction of the facility housing the USDA/NFC CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as facility guards, access controls, and 24/7 surveillance, shall provide robust protection against unauthorized access to the USDA/NFC CA equipment and records.

#### **5.1.2 Physical Access**

The USDA/NFC CA equipment shall always be protected from unauthorized access, especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

These security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the USDA/NFC CA plans to issue certificates at all levels of assurance, it shall be operated and controlled on the presumption that it will be issuing at least one High Assurance certificate, the requirements of which include, but are not limited to:

- ?? Ensuring no unauthorized access to the hardware is permitted
- ?? Ensuring all removable media and paper containing sensitive plain-text information be stored in secure containers
- ?? Manually or electronically monitoring for unauthorized intrusion at all times;
- ?? Ensuring an access log be maintained and inspected periodically; and
- ?? Establishing two person entry mechanisms.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, USDA/NFC CA equipment shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the USDA/NFC CA equipment (operating at the Basic Assurance level or higher) shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- ?? The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the USDA/NFC CA, that all equipment other than the repository is shut down);
- ?? Any security containers are properly secured;
- ?? Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- ?? The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

### **5.1.3 Electrical Power**

The USDA/NFC CA (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The USDA/NFC CA directories (containing USDA/NFC CA issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for continuous operation in the absence of commercial power, to support a smooth shutdown of the main USDA/NFC CA facility, while switching operations to its alternative “warm site”.

### **5.1.4 Water Exposures**

USDA/NFC CA shall be located in a computer room designed to minimize exposure to water. Moisture/water detectors shall be installed in areas susceptible to flooding, and shall be monitored 24/7 by computer operations personnel.

### **5.1.5 Fire Prevention and Protection**

USDA/NFC CA shall be located in a computer room utilizing a “dry pipe” fire protection system. Fire (smoke) sensors/monitors shall be located throughout the computer room, and shall be monitored 24/7 by computer operations personnel. Fire extinguishers shall be located throughout the computer room, and in the immediate vicinity of the USDA/NFC PKI/CA equipment. In addition, there shall be an onsite Fire Department (managed by the facility contractor) to provide fire safety and prevention mechanisms including alarms and fire extinguishers. These alarms and extinguishers shall be inspected monthly.

### **5.1.6 Media Storage**

USDA/NFC CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the USDA/NFC CA.

### **5.1.7 Waste Disposal**

No stipulation.

### **5.1.8 Off-site Backup**

For the USDA/NFC CA (operating at the Basic Assurance level or higher), full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups shall be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the USDA/NFC CA equipment). Only the latest full backup shall be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational USDA/NFC CA.

## **5.2 PROCEDURAL CONTROLS FOR THE USDA/NFC CA**

### **5.2.1 Trusted Roles**

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles shall be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the USDA/NFC CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are therefore drawn in terms of five, somewhat abstract, roles (Note: the information derives from the Certificate Issuing and Management Components Protection Profile being developed by NIST.) :

**Operational Authority Administrator** - authorized to install, configure, and maintain the CA, establish and maintain CA system accounts, configure profiles and audit parameters, and generate component keys.

**Operational Authority Officer/RA** - authorized to create, recover and revoke user and device certificates. Responsible for maintaining the user and device authentication documentation.

**LRA** - authorized to request or approve certificates or certificate revocations.

**Auditor** - authorized to maintain, review and archive audit logs and audit parameters.

**Operator** - authorized to perform routine operation of the CA equipment, and system backup and recovery.

#### **5.2.1.1 Operational Authority Administrator**

The administrator role shall be responsible for:

- ?? Installing, configuring, and maintaining the CA
- ?? Establishing and maintaining CA system accounts
- ?? Configuring certificate profiles, templates and audit parameters
- ?? Generating and backing up CA keys

Administrators shall not issue certificates to subscribers.

#### **5.2.1.2 Operational Authority Officer/RA**

The officer role shall be responsible for:

- ?? Creating the Users Certificate from information furnished by the LRA
- ?? Executing the issuance, revoking and recovery of certificates
- ?? Maintaining a file of the original signed request and subscriber information
- ?? Archiving the original documentation to long term storage annually
- ?? Distributing subscribers authorizations, reference numbers or partial shared secret portions to the appropriate Subscriber Organization end entities

#### **5.2.1.3 LRA**

The LRA role shall be responsible for:

- ?? Registering new subscribers and requesting the issuance of certificates
- ?? Verifying the identity of subscribers and accuracy of information included in certificates
- ?? Requesting and approving the revocation of certificates
- ?? Submitting the original signed request, subscriber agreement and authentication documentation (pictured ID's) to the NFC PKI Officers
- ?? Receiving their subscribers' authorization codes via encrypted e-mail or document from the NFC PKI RA and communicates that information to their subscriber in a secure manner other than e-mail
- ?? Instructing their subscribers regarding the download, where applicable, and/or activation of subscriber certificates

#### **5.2.1.4 Auditor**

The auditor role shall responsible for:

- ?? Reviewing audit logs and audit parameters
- ?? Performing or overseeing internal compliance audits to ensure that the USDA/NFC CA is operating in accordance with its CPS
- ?? Maintaining and archiving audit logs

### **5.2.1.5 Operator**

The operator role shall be responsible for:

?? The routine operation of the CA equipment and operations

?? System backups and recovery or changing recording media

### **5.2.2 Separation of Roles**

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

The separation of roles for the USDA/NFC CA's shall be as follows:

<b>Assurance Level</b>	<b>Role Separation Rules</b>
Basic	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.
Medium	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume an Officer role may not assume an Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, or an Auditor and an Officer role. No individual shall be assigned more than one identity.
High	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA system shall identify and authenticate its users and shall ensure that no user identity can:  ?? Assume both the Administrator and Officer roles  ?? Assume both the Administrator and Auditor roles  ?? Assume both the Auditor and Officer roles.  No individual shall have more than one identity.

The USDA/NFC CA shall operate at the High Assurance level.

### **5.2.3 Number of Persons Required Per Task**

To best ensure the integrity of the USDA/NFC CA equipment and operation, no individual will be assigned more than one trusted role. The separation provides a set of checks and balances over the USDA/NFC CA operation.

Under no circumstances shall the incumbent of a USDA/NFC CA role perform its own auditor function.

### **5.2.4 Identification and Authentication for Each Role**

At all assurance levels, an individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

## **5.3 PERSONNEL CONTROLS**

### **5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements**

The individuals responsible and accountable for the operation of the USDA/NFC CA are the USDA/NFC PKI Policy Authority and the USDA/NFC CA OA.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS.

USDA/NFC CA personnel shall hold Limited Background Investigation (LBI) security clearances.

### **5.3.2 Background Check Procedures**

Agency background check procedures shall be described in the CPS and shall demonstrate that Agency requirements set forth in Section 5.3.1 are met.

### **5.3.3 Training Requirements**

All personnel performing duties with respect to the operation of the USDA/NFC CA shall receive comprehensive training. Training shall be conducted in the following areas:

- ?? CA/RA/LRA security principles and mechanisms
- ?? All PKI software versions in use on the CA system
- ?? All PKI duties they are expected to perform
- ?? Disaster recovery and business continuity procedures.

Documentation shall be maintained identifying all personnel who received formal training and the level of that training completed.

#### **5.3.4 Retraining Frequency and Requirements**

Individuals responsible for PKI roles shall be aware of changes in the USDA/NFC CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are USDA/NFC CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

#### **5.3.5 Job Rotation Frequency and Sequence**

No stipulation.

#### **5.3.6 Sanctions for Unauthorized Actions**

The USDA/NFC PKI Operational Authority will refer to the appropriate authority for appropriate administrative and disciplinary actions against personnel who have performed actions involving the USDA/NFC CA or its repository .

#### **5.3.7 Contracting Personnel Requirements**

Contractor personnel employed to perform functions pertaining to the USDA/NFC CA shall meet applicable requirements set forth in the USDA/NFC CA CPS as determined by the USDA/NFC CA OA or the contracting Agency.

#### **5.3.8 Documentation Supplied to Personnel**

The USDA/NFC CA shall make available to its CA, RA and LRA personnel the certificate policies it supports, relevant parts of the CPS, and any relevant statutes, policies or contracts. .

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1 KEY PAIR GENERATION AND INSTALLATION**

#### **6.1.1 USDA/NFC CA and CA Key Pair Generation**

Cryptographic keying material for certificates issued by the USDA/NFC CA shall be generated in FIPS 140 validated cryptographic modules. For the USDA/NFC CA, the modules shall meet or exceed Security Level 3.

#### **6.1.2 Private Key Delivery to Subscriber**

The USDA/NFC CA generates its own key pair and therefore does not need private key delivery. For encryption keys, delivery of the private key to the Subscriber shall be in accordance with the requirements of this CP and the CPS.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

Public keys shall be delivered to the certificate issuer in an authenticated manner set forth in the USDA/NFC CA CPS. This is usually via a certificate electronic request message from a RA, but it may also be done through other secure electronic mechanisms. Further, it may be accomplished via secure non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. If off-line means are used, they shall include identity checking as set forth in this CP and shall also ensure that proof of possession of the corresponding private key is accomplished.

#### **6.1.4 USDA/NFC CA Public Key Delivery to Subscriber Certificate Holder's**

The Public Key corresponding to the USDA/NFC CA's private signing key shall be delivered to end entities protected by PKIX-CMP. The USDA/NFC CA can affect delivery by on-line transactions or other appropriate mechanisms.

#### **6.1.5 Key Sizes**

All FIPS-approved signature algorithms shall be considered acceptable. If the USDA/NFC PKI Policy Authority determines that the security of a particular algorithm may be compromised, it may require the USDA/NFC CA's to revoke the affected certificates (in the latter case, in order to support continued compliance with the MOA).

All certificates issued by the USDA/NFC CA shall use at least 1024 bit Rivest-Shamir-Adleman encryption algorithm (RSA) or Digital Signature Algorithm (DSA), with Secure Hash Algorithm version 1 (SHA-1) or better. Use by the USDA/NFC CA or an Agency of SSL or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys.

### 6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

### 6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186, and additional tests if specified by the USDA/NFC PKI Policy Authority.

### 6.1.8 Hardware/Software Subscriber Key Generation

For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys, as set forth in the table below. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

Assurance Level	Key Generation Mechanism
Basic	Software or Hardware
Medium	Software or Hardware
High	Hardware only

### 6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalsignature* and *nonrepudiation* bits. Certificates to be used for data encryption shall set the *dataencryption* bit. USDA/NFC CA certificates shall set two key usage bits: *cRLSign* and *CertSign*. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management certificates.

## 6.2 PRIVATE KEY PROTECTION

### 6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* latest version of FIPS 140 series. However, the USDA/NFC PKI PA may determine that other comparable validation, certification, or verification standards are sufficient. If so, those standards will be published by the USDA/NFC PKI PA. Cryptographic modules shall be validated to the latest version of the FIPS 140 series level identified in this section, or validated, certified, or verified to requirements published by the USDA/NFC PKI Policy Authority. Additionally, cryptographic modules used by the USDA/NFC CA shall be designed and manufactured by companies approved by the USDA/NFC PKI Policy Authority.

The table below summarizes the minimum requirements for USDA/NFC cryptographic modules:

<b>Assurance Level</b>	<b>Latest version of FIPS 140 series</b>	<b>USDA/NFC Certification Authority</b>	<b>Subscriber</b>	<b>Registration Authority</b>
<b>Basic</b>	Required	Level 3 (Hardware)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
<b>Medium</b>	Required	Level 3 (Hardware)	Level 1 (Hardware or Software)	Level 2 (Hardware)
<b>High</b>	Required	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

### **6.2.2 USDA/NFC CA Private Key Multi-person Control**

Use of the USDA/NFC CA private signing key shall require action by multiple persons as set forth in Section 5 of this CP.

### **6.2.3 Key Escrow of USDA/NFC CA Private Signature Key**

Under no circumstances shall the USDA/NFC CA signature keys used to support non-repudiation services be escrowed by a third party.

### **6.2.4 Private Key Backup**

#### **6.2.4.1 Backup of USDA/NFC CA Private Signature Key**

The USDA/NFC CA and subscriber roaming private signature keys shall be backed up under the same multi-person control as the original signature key. One backup shall be kept at the USDA/NFC CA facility, and another backup copy shall be kept at the alternate “warmsite”. Procedures to effect this shall be included in the CPS.

Additionally, the NFC/CA is structured in a high availability configuration with a primary and secondary system for backup as necessary.

#### **6.2.4.2 Backup of Subscriber Private Signature Key**

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the USDA/NFC CA medium Assurance or basic Assurance policies may be backed up or copied, but shall be held in the Subscriber’s control.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the USDA/NFC CA high Assurance policy shall not be backed up or copied.

### **6.2.5 Private Key Archival**

Local private signature keys shall not be backed up, escrowed, or copied.

### **6.2.6 Private Key Entry into Cryptographic Module**

USDA/NFC CA private keys shall be generated by and remain in a cryptographic module. The CA private keys may be backed up in accordance with Section 6.2.4.1.

### **6.2.7 Method of Activating Private Keys**

The subscriber shall be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

### **6.2.8 Methods of Deactivating Private Keys**

If cryptographic modules are used to store subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

### **6.2.9 Method of Destroying Subscriber Private Signature Keys**

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware should not be required.

## **6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT**

A subscriber’s key-pair that is used for digital signatures shall never be escrowed, archived or backed up, because a subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the subscriber shall use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the subscriber departs the Agency without relinquishing the private key or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, a Subscriber Organization shall be able to escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs shall be employed.

### **6.3.1 Public Key Archival**

The public key is archived as part of the certificate archival.

### **6.3.2 Usage Periods for the Public and Private Keys**

The USDA/NFC CA private signing keys shall be used to sign certificates for not more than one-half the certificate life. The certificates the USDA/NFC CA issues shall be valid for not more than 10 years.

## **6.4 ACTIVATION DATA**

### **6.4.1 Activation Data Generation and Installation**

The activation data used to unlock USDA/NFC CA or subscriber private keys, in conjunction with any other access control mechanisms, shall be protected at a level appropriate to the strength of the keys and/or data being protected. It shall satisfy the policy enforced at/by the cryptographic module. Where pass phrases are used as activation data, the pass phrases shall be generated in conformance with FIPS-112.

### **6.4.2 Activation Data Protection**

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be memorized and not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

### **6.4.3 Other Aspects of Activation Data**

No stipulation.

## **6.5 COMPUTER SECURITY CONTROLS**

### **6.5.1 Specific Computer Security Technical Requirements**

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The USDA/NFC CA and its ancillary parts shall include the following functionality:

- ?? Require authenticated logins;
- ?? Provide Discretionary Access Control;
- ?? Provide a security audit capability;
- ?? Restrict access control to USDA/NFC CA services and PKI roles;
- ?? Enforce separation of duties for PKI roles;
- ?? Require identification and authentication of PKI roles and associated identities;

- ?? Prohibit object re-use or require separation for USDA/NFC CA random access memory;
- ?? Require use of cryptography for session communication and database security;
- ?? Archive USDA/NFC CA history and audit data;
- ?? Require self-test security related USDA/NFC CA services;
- ?? Require a trusted path for identification of PKI roles and associated identities;
- ?? Require a recovery mechanisms for keys and the USDA/NFC CA system; and
- ?? Enforce domain integrity boundaries for security critical processes.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer system as that which received the evaluation rating.

### **6.5.2 Computer Security Rating**

No Stipulation.

## **6.6 LIFE-CYCLE TECHNICAL CONTROLS**

### **6.6.1 System Development Controls**

The System Development Controls for the USDA/NFC CA are as follows:

- ?? The USDA/NFC CA shall use software that has been designed and developed under a formal, documented development methodology.
- ?? Hardware and software procured to operate the USDA/NFC CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- ?? Hardware and software developed for the USDA/NFC CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- ?? All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the USDA/NFC CA physical location.
- ?? The USDA/NFC CA hardware and software shall be dedicated to performing one task: the USDA/NFC CA. There shall be no other applications, hardware devices, network connections, or component software installed which are not part of the USDA/NFC CA operation.
- ?? Proper care shall be taken to prevent malicious software from being loaded onto the USDA/NFC CA equipment. Only applications required to perform the operation of the USDA/NFC CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

?? Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

### **6.6.2 Security Management Controls**

The configuration of the USDA/NFC CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the USDA/NFC CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the USDA/NFC CA system. The USDA/NFC CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. For the USDA/NFC CA, the integrity of the software shall be verified by the USDA/NFC CA OA at least once a week (e.g., in conjunction with CRL publication).

### **6.6.3 Life Cycle Security Ratings**

No stipulation.

## **6.7 NETWORK SECURITY CONTROLS**

The USDA/NFC CA and USDA/NFC Internal Directory shall be connected within a USDA/NFC secure network segment. The USDA/NFC CA Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). Information will be transported from the Internal Directory to the Border Directory using an automated mechanism.

The USDA/NFC CA shall employ appropriate security measures to ensure it is guarded against denial of service and intrusion attacks. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA.

The USDA/NFC CA CPS shall define the network protocols and mechanisms required for the operation of the USDA/NFC Border Directory CA. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

## **6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

Requirements for cryptographic modules are as stated above in Section 6.2

## 7. CERTIFICATE AND CRL PROFILES

### 7.1 CERTIFICATE PROFILE

#### 7.1.1 Version Numbers

The USDA/NFC CA shall issue X.509 v3 certificates.

#### 7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions shall be defined in profiles. Certificate extensions used by the USDA/NFC CA shall conform to the Federal certificate profile established by NIST. These profiles shall be written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CA's and communities. Medium and Basic Assurance Level certificates shall use *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile*. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

#### 7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OID's for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates under this CP will use the following OID's for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Certificates containing keys generated for use with DSA or for use with KEA shall be signed with id-dsa-with-sha1. Keys generated for use with RSA shall be signed using sha-1WithRSAEncryption.

#### **7.1.4 Name Forms**

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name as specified in FPKI-PROF, with the attribute type as further constrained by [RFC2459].

#### **7.1.5 Name Constraints**

No stipulation.

#### **7.1.6 Certificate Policy Object Identifier**

Certificates issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued, as described in 1.2 of this CP.

#### **7.1.7 Usage of Policy Constraints Extension**

No stipulation.

#### **7.1.8 Policy Qualifiers Syntax and Semantics**

Certificates issued under this CP shall not contain policy qualifiers.

#### **7.1.9 Processing Semantics for the Critical Certificate Policy Extension**

Processing semantics for the critical certificate policy extension used by the USDA/NFC CA shall conform to FPKI-PROF.

### ***7.2 CRL PROFILE***

#### **7.2.1 Version Numbers**

The USDA/NFC CA shall issue X.509 version two (2) CRL's.

#### **7.2.2 CRL Entry Extensions**

Detailed CRL profiles addressing the use of each extension shall conform to FPKI-PROF.

## **8. SPECIFICATION ADMINISTRATION**

### **8.1 SPECIFICATION CHANGE PROCEDURES**

The USDA/NFC PKI Policy Authority shall review this CP at least once every year. The USDA/NFC PKI Policy Authority shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP shall be communicated to every CA and Subscriber. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the USDA/NFC PKI Policy Authority shall be disseminated to interested parties. All interested parties shall provide their comments to the USDA/NFC PKI Policy Authority in a fashion to be prescribed by the USDA/NFC PKI Policy Authority.

In evaluating the need for changes to this CP and the Object Identifiers it contains, the USDA/NFC PKI Policy Authority will be guided by the language of RFC 2527, which states (in section 4.8.1):

*It will occasionally be necessary to change certificate policies and Certification Practice Statements. Some of these changes will not materially reduce the assurance that a certificate policy or its implementation provides, and will be judged by the policy administrator as not changing the acceptability of certificates asserting the policy for the purposes for which they have been used. Such changes to certificate policies and Certification Practice Statements need not require a change in the certificate policy Object Identifier or the CPS pointer (URL). Other changes to a specification will change the acceptability of certificates for specific purposes, and these changes will require changes to the certificate policy Object Identifier or CPS pointer (URL).*

### **8.2 PUBLICATION AND NOTIFICATION POLICIES**

This CP and any subsequent changes shall be made publicly available within one week of approval.

### **8.3 CPS APPROVAL PROCEDURES**

The term Certification Practice Statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding certificate policy described above. The USDA/NFC CA CPS, which is contained in a separate document published by the USDA/NFC CA OA and approved by the USDA/NFC PKI Policy Authority, specifies how the USDA/NFC CA CP will be implemented to ensure compliance with its provisions in accordance with the USDA/NFC CA OA.



## 9. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

- ABADSG      Digital Signature Guidelines, 1996-08-01.  
<http://www.abanet.org/scitech/ec/isc/dsgfree.html>.
- FBCA          Federal Bridge Certification Authority (FBCA) Version 1.12, 2000-12-17  
<http://>
- FIPS 112      Password Usage, 1985-05-30  
<http://csrs.nist.gov/fips/>
- FIPS 140-1   Security Requirements for Cryptographic Modules, 1994-01  
<http://csrs.nist.gov/fips/fips1401.htm>
- FIPS 186      Digital Signature Standard, 1994-05-19  
<http://csrs.nist.gov/fips/fips186.pdf>
- FOIACT      5 U.S.C. 552, Freedom of Information Act.  
[Http://www4.law.cornell.edu/uscode/5/552.html](http://www4.law.cornell.edu/uscode/5/552.html)
- FPKI-Prof    Federal PKI X.509 Certificate and CRL Extensions Profile  
<http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls>
- ISO9594-8   Information Technology-Open Systems Interconnection-The Directory:  
Authentication Framework, 1997.  
<ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc>
- ITMRA       40 U.S.C. 1452, Information Technology Management Reform Act of 1996.  
[Http://www4.law.cornell.edu/uscode/40/1452.html](http://www4.law.cornell.edu/uscode/40/1452.html)
- NAG69C      Information System Security Policy and Certification Practice Statement for  
Certification Authorities, rev C, November 1999.
- NSD42       National Policy for the Security of National Security Telecom and  
Information Systems, 5 Jul 1990.  
[Http://snyside.sunnyside.com/cpsr/privacy/computer\\_security/nsd\\_42.txt](http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt)  
(redacted version)
- NS4005      NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August  
1997.
- NS4009      NSTISSI 4009, National Information Systems Security Glossary, January  
1999.
- PKCS#12     Personal Information Exchange Syntax Standard, April 1997.  
[Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html](http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html)
- RFC 2510     Certificate Management Protocol, Adams and Farrell, March 1999.
- RFC 2527     Certificate Policy and Certificate Practices Framework, Chokhani and Ford,  
March 1999.

Security Requirements for Certificate Issuing and Management Components,  
3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0,  
13 December 1999

## 10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certificate Authority
USDA/NFC CA	USDA/NFC Certification Authority
USDA/NFC CA OA	USDA/NFC Certification Authority Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
LRA	Local Registration Authority
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the USDA/NFC PKI Policy Authority allowing interoperation

	between the USDA/NFC CA and Agency Principal CA)
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCFO	Office of the Chief Financial Officer
OID	Object Identifier
OGC	Office of General Counsel
OMB	Office of Management and Budget
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UMARS	User Management and Registration Systems
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
USDA	United States Department of Agriculture
WWW	World Wide Web

## 11. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity recognized by the USDA/NFC PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance

---

	with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRL's.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

---

CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to being associated with an operator or administrator.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the

---

	private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate, which is composed of two subfields: "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Agency as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
United States Department of Agriculture and National Finance Center (USDA/NFC)	The United States Department of Agriculture and National Finance Center Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Agency Principal Certification Authorities.
United States Department of Agriculture and National Finance Center Certification Authority Membrane	The United States Department of Agriculture and National Finance Center Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directories, External Directories, Firewalls, Routers, Randomizers, etc.

---

USDA/NFC CA OA (OA)	The USDA/NFC CA OA is the organization selected by the USDA/NFC PKI PA to be responsible for operating the USDA/NFC CA.
USDA/NFC Public Key Infrastructure Policy Authority (USDA/NFC PKI PA)	The USDA/NFC PKI PA is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the USDA/NFC CA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract

---

	binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the USDA/NFC PKI Policy Authority and an Agency allowing interoperability between the Agency and the USDA/NFC CA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DN's) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral

	part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the three policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the USDA/NFC CA, the PMA is the USDA/NFC PKI Policy Authority.
Principal CA	The Principal CA is a CA designated by an Agency to interoperate with the USDA/NFC CA. An Agency may designate multiple Principal CA's to interoperate with the USDA/NFC CA.
Privacy	Restricting access to subscriber or Agency (Relying Party) information in accordance with Federal law and Agency policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

---

Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

## **12. ACKNOWLEDGEMENTS**

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 1.12

